強連結オートマトンとその商オートマトンの自己同型群(計算量理論の諸相 : その基礎的研究)

AUTHOR(S):

植村, 憲治

CITATION:

植村, 憲治. 強連結オートマトンとその商オートマトンの自己同型群(計算量理論の諸相 : その基礎的研究). 数理解析研究所講究録 1996, 943: 97-105

ISSUE DATE:

1996-04

URL:

http://hdl.handle.net/2433/60163

数理解析研究所講究録
943巻 1996年 97-105

強連結オートマトンとその商オートマトンの自己同型群

都留文科大学　植村憲治　(Kenji Uemura)

あらまし　強連結オートマトンAにおける構造半群$\mathcal{C}(A)$の極小べき等元eから得られる群$e\mathcal{C}(A)e$は，Aの自己同型群$\mathcal{A}(A)$と重要なかかわりを持っていることが知られている[10,11]．本稿では$e\mathcal{C}(A)e$を用いて，Aの自己同型群構成に関する結果を示す．

強連結オートマトンAの自己同型群は，$e\mathcal{C}(A)e$の部分群の準同型像となることが知られている[10,11]．特に極小べき等元による状態集合の像$\{Xe\}\ e\in E_0$(E_0は極小べき等元全体の集合)が，状態集合の分割を導く時には，$e\mathcal{C}(A)e$の中心化群と同型になる．本稿ではまずこれらの結果を，$\{Xe\}$が状態集合の被覆となっている場合に拡張させることを考える．そのために基本分割の概念を導入する．そしてXe上の置換群$e\mathcal{C}(A)e$の中心化群の元で，Xeに属する基本分割の同値類を固定しているものの全体が，$\mathcal{A}(A)$と同型になることを示す．

これはBarnes[1]による自己同型群となるための条件をより具体的に述べたもので，自己同型群の有効的な構成方法を得るための手掛かりを与えるものとなっている．

キーワード　代数的オートマトン理論，オートマトンの自己同型群，構造半群，有限半群，極小べき等元

1．まえがき

有限オートマトンの分解は有限オートマトンを，より単純ないくつかの有限オートマトンの積で表現しようとするもので，代数的オートマトン理論における重要なテーマである．

eを強連結オートマトン$A=(X,I,M)$の構造半群$e\mathcal{C}(A)e$の極小べき等元とする

時，$\mathcal{A}(A)$は$e\mathcal{C}(A)e$の部分群の準同型像となる(10,11)．また極小べき等元による像の集合がXの分割を与える場合には，$\mathcal{A}(A)$は，Xe上の置換群$e\mathcal{C}(A)e$の中心化群と同型になる．更に，このとき$\#e\mathcal{C}(A)e = \#Xe$であれば，$\mathcal{A}(A)$は$e\mathcal{C}(A)e$と同型になる(11)．

$T_X=\{u\in I^* | N(x,u)=x\}$ と定めると，強連結オートマトンの場合は，$\mathcal{A}(A)$が正則置換群になることより，$\mathcal{A}(A)$による分割において同じ同値類に属する任意の状態x,yは$T_X=T_y$を満たす(即ち等しい固定半群をもつ)．Barnes(1)はこの逆について調べ，構造半群による変換が同値関係を保存する分割で，同じ同値類に属する任意の状態x,yが等しい固定半群をもつような最大の分割が$\mathcal{A}(A)$による分割と等しいことを示した．しかしながらこれらの方法は$\mathcal{A}(A)$を求める具体的方法には触れていない．

３章ではXe上の置換群$e\mathcal{C}(A)e$の中心化群の元で，基本分割と名付けたX上の分割のXeに含まれる同値類の元を，その同値類の中で動かすものの全体が$\mathcal{A}(A)$と同型になることを示す．

３章の結果は，Fleck(6)，Perrin et Perrot(８)と植村 (10,11) の結果の拡張であり，有限強連結オートマトンの自己同型群を，極小べき等元の像による頂点被覆が分割になっていない場合にも特徴付けたことになる．また，Barnes(1)による自己同型群の記述をより具体的に示したものとなっている．

２．準備

[定義] Xを状態の空でない有限集合，Iを記号の空でない有限集合，NをX×Iから Xへの写像とする三項対A=(X,I,N)を（**有限**）**オートマトン**という．

I^*をIの記号による全ての記号列の集合とし，λを空語とすると，全てのu,v $\in I^*$と全てのx∈Xに対して$N(x,uv)=N(N(x,u),v)$を満たすようにNの領域をX×I^*へ拡張することが出来る．

[定義] オートマトンA=(X,I,N)が**強連結**とは，任意のx,y∈Xに対して，y =N(x,u)となるu∈I^*が存在する場合をいう．

[定義] Aをオートマトンとする．X上の置換gがAの**自己同型写像**とは，全てのx∈Xとu∈Iに対してN(x,u)g=N(xg,u) が成り立つときをいう．Aの自己同型写像の全体はX上の置換群となる．これを$\mathcal{A}$(A)で表す．

[定義] u∈I^*−{λ}は，X上の写像$x\cdot\phi_u=N(x,u)$を導く．半群$\mathcal{C}(A)=\{\phi_u \mid u\in I^*-\{\lambda\}\}$ をAの**構造半群**と呼ぶ．

[定義] $xg^n=x$となる正整数nとx∈Xが存在するなら$g^n=id$（恒等置換）となるX上の置換gを，**正則置換**という．置換群Gの全ての要素が正則置換であるときGを**正則置換群**という．

[定義] x∈XとX上の置換群Gに対して，xGをxのGによる**可遷域**と言う．ただ一つの可遷域からなる置換群を**可遷置換群**と言う．このとき，任意のx,y∈Xに対してy=xgとなるg∈Gが存在する．

gが強連結オートマトンAの自己同型写像で$xg^n=x$とすれば，$yg^n=N(x,u)g^n=N(xg^n,u)=N(x,u)=y$となってgは正則である．すなわち強連結オートマトンの自己同型群はX上の正則置換群となる．

[定義] X上の置換群GとXの点xに対して，Gの部分群$G_X=\{g\in G \mid xg=x\}$をGのx-**固定部分群**（１３）と呼ぶ．

Fix(x,G)でG_Xにおける不動点集合$\{y\in X \mid yg=y \text{ for any } g\in G_X\}$を表す．同様にXの上の写像による半群Sにおいて，Sのx-固定部分半群S_Xと不動点集合Fix(x,S)が定義される．

[定義] Gを有限集合X上の置換群とする．任意のg∈GとX∈Xに対してx(hg)=x(gh)となる置換hの集合は置換群となり，Gの**中心化群**と呼ばれる．

X上の可遷置換群Gの中心化群Hは，各々のG_Xの不動点集合を可遷域とする正則置換となる（１３）．即ちxH=Fix(x,G)が成り立つ．

x,y∈X,g∈$\mathcal{A}$(A),u∈I^*に対して,xg=y，N(x,u)=xが成り立てばN(y,u)=N(xg,u)=N(x,u)g=xg=yとなる．これから，$\mathcal{C}(A)_X=\mathcal{C}(A)_y$は，y=xgとなる自己同型写像gが存在するための必要条件となっていることが判る．言い換えれば，自己同型群は構造半群の同じ固定部分半群を持つ頂点上の正則置換

群となっている．

[定理１(１５)Cayleyの定理]Gを任意の群とする．G上の置換g_Rを$hg_R=hg$ $(h\in G)$で定めると，$G_R=\{g_R \mid g\in G\}$はG上の可遷正則置換群となり，写像ϕ: $g\mapsto g_R$によってGと同型になる．同様にg_Lを，$hg_L=g^{-1}h(h\in G)$と定めると，G_L $=\{g_L \mid g\in G\}$はG上の可遷正則置換群となり，写像$\psi: g\mapsto (g^{-1})_L$によってGと同型になる．

[系１] GをX上の可遷正則置換群とする．このときGと同型なX上の可遷正則置換群Sで，任意の$g\in G$，$s\in S$に対して$sg=gs$が成り立つものがただ一つ存在する．

強連結オートマトンAの自己同型群を求めることは，Aの構造半群をX上の適当な部分集合上に制限させて，そこでの可遷正則置換群を求める問題に帰着する．３章ではこの手法によるこれまでの成果と，中心化群を用いる方法について述べる．

３．極小べき等元と強連結オートマトン

[定義] 半群Sの元eが$e^2=e$をみたすとき，eはべき等元と呼ばれる．EでSのべき等元全体の集合を表す．$e_i,e_j\in E$に対して，$e_i\leqq e_j$とは$e_ie_j=e_je_i=e_i$が成り立つときと定めると，$\leqq$はE上の半順序になる．

[補題１] sを有限半群Sの任意の元とする．このときs^nがべき等元となる正整数nが存在する．

[定義] $e\in E$が，$e'\in E$に対して$e'\leqq e$なら$e'=e$となるとき，eを**極小べき等元**という．

[定理２](4,１１)Sを有限半群，eをSのべき等元とする．部分半群eSeが群となる必要十分条件はeが極小であることであり，この群は同型を除いて一意である．

[補題２(１１)] e_1を有限集合X上の写像による半群Sの極小べき等元とする．べき等元e_2が極小であるための必要十分条件は$\#Xe_1=\#Xe_2$が成り立つことで

ある．

［補題3］eを有限集合X上の写像による半群Sの極小べき等元とする．aをSの任意の元とするとX(ea)^n＝X(ea)となる極小べき等元(ea)^{n}が存在する．

証明略．

［定理３(１１)］Sを有限集合X上の写像による可遷半群，eをSの極小べき等元とすれば(Xe)･eSe＝Xeとなる．すなわちeSeをXeに制限したものはeSeと同型であり，Xe上の置換群となる．また，E_0＝｛$e_0,e_2,\ldots,e_{m-1}$｝をSの全ての極小べき等元の集合とするとこれは部分半群となり，$\cup_{e\in E_0}Xe=X$を満たす．

Sを有限集合X上の写像による可遷半群とする．x，y∈Xに対してxR_0yを”x∈Xe⇔y∈Xeが全てのe∈E_0に対して成り立つとき，”と定めればR_0は同値関係となり，X上の分割を導く．また補題３より，任意のa∈Sに対してxR_0yならば，xaR_0yaが成り立つ．

［定義］xRyを，”xR_0yであって，x＝xeとなる任意のe∈E_0と，x＝x'e，y＝y'e,x'，y'∈Xe'，e'∈E_0となる全てのe',x',y'に対してx'R_0y'が成り立つ場合,”と定めると，このRはR_0の細分となる．RによるXの分割をSによる基本分割と呼ぶ．作り方より基本分割の同値類は，あるXeに含まれる．言い換えれば任意のXe（e∈E_0）はRのいくつかの同値類の和集合となる．

［補題4］SをX上の可遷半群とする．$S_X=S_y$ならば，xとyは基本分割上の同じ同値類に属する．

（証明）対偶を示す．x,yがRの異なる同値類に属するとする．xR_0yが成り立たない時，即ちx∈Xe，y∉Xeとなるe∈E_0が存在するならe∈S_X，e∉S_yとなって，$s_X\neq s_y$である．xR_0yが成り立ち，かつx＝x'e，y＝y'eとなるx',y'∈Xe'(e，e'∈E_0）で，x'R_0y'が成り立たないものがある場合を考える．このとき，x'∈Xe”∩Xe'，y'∉(Xe”∩Xe')となるe”∈E_0が存在する．x'＝x”e'とx”∈Xeとなるx”に対してSが可遷ゆえ，x”＝xaeとなるx∈Xe，a∈Sが存在する．故にx＝x'e＝x'e”e＝x”e'e”e＝xaee'e”eとなってaee'e”e∈S_Xが成り立つ．xR_0yゆえ，yaee'e”∈Xe”∩Xe'となり，yaee'e”≠y'である．eは，

Xe'からXeへの全単射ゆえ，yaee'e"e≠yとなって， aee'e"e$\notin S_y$となる．故に$S_x \neq S_y$が成り立つ．□

即ち強連結オートマトンの自己同型群は，基本分割の同値類を固定した置換と言う性質，即ち可遷域が基本分割の同値類に含まれると言う性質と，Xe上の置換群e$\mathcal{C}$(A)eと可換と言う二つの性質をもつ． 本論文の主定理はこれについて述べた次の定理である．

［定理４］A=(X,I,N)を強連結オートマトン，e_0を構造半群$\mathcal{C}$(A)の極小べき等元とする．Aの自己同型群は，Xe_0上の群$e_0\mathcal{C}(A)e_0$の中心化群の要素で，Xe_0に含まれる基本分割の同値類を固定しているものからなる部分群H'に同型である．

（証明）H'が部分群となることは明らかである．$Xe_0=Q_1 \cup Q_2 \cup \ldots \cup Q_n$，$Q_i \cap Q_j = \phi$ (i≠j)，Q_i (1≦i≦n) は基本分割の同値類とする．h'∈H'に対して$Q_i h' = Q_i$が (1≦i≦n) 成り立つ．以下において，H'をXに拡張し，その元が構造半群の元と可換であること示す．

$\phi_{ij}: Xe_i \to Xe_j$ (0≦i,j≦m-1, e_i, $e_j \in E_0$) を$x\phi_{ij} = xe_j$と定める．このϕ_{ij}は全単射となって逆写像が存在する．また$x \in Xe_i \cap Xe_j$のとき，$x\phi_{ij} = x$と，$x\phi_{ik} = x\phi_{jk}$ (0≦k≦m-1) が成り立ち，$y \in (Xe_i \cap Xe_j)\phi_{ik}$のとき，$y\phi_{ik}^{-1} = y\phi_{jk}^{-1}$が成り立つ．

h'∈H'に対してX上の置換hを次のように定める．x∈Xe_i (0≦i≦m-1) の時，$xh \equiv x\phi_{i0}h'\phi_{i0}^{-1}$．h'が基本分割の同値類を固定することから，この値は定まる．$x \in Xe_i \cap Xe_j$の時，$xh = x\phi_{i0}h'\phi_{i0}^{-1} = xe_0h'\phi_{i0}^{-1} = x\phi_{j0}h'\phi_{i0}^{-1} = x\phi_{j0}h'\phi_{j0}^{-1}$となってhはX上の置換となる．任意のg',h'に対して$x(gh) = (xg)h = (xg')h' = (x\phi_{i0}g\phi_{i0}^{-1})\phi_{i0}h\phi_{i0}^{-1} = x\phi_{i0}gh\phi_{i0}^{-1} = \phi_{i0}(gh)'\phi_{i0}^{-1}$となる．また$x \in Xe_0$のときは，hはh'と等しい．よってHは，H'の拡張となり，HとH'は同型である．

次に，このhが$\mathcal{C}$(A)の元と可換であることを示す．x∈Xe_i，u∈$\mathcal{C}$(A)，h'∈H'，xu∈Xe_j，x=ye_i，y∈Xe_0とする．$xuh = ye_iuh = ye_iu\phi_{j0}h'\phi_{j0}^{-1} =$

$y(e_0e_iue_0)h'\phi_{j0}^{-1}=yh'(e_0e_iue_0)\phi_{j0}^{-1}=yh'e_iue_0\phi_{j0}^{-1}\cdots(*)$.
h'がXe_0に含まれる基本分割の同値類を固定し，yとyh'は基本分割の同じ同値類に属することと，$ye_iuR_0yh'e_iu$が成り立つことより，$(*)=yh'e_iu\phi_{j0}\phi_{j0}^{-1}=yh'e_0e_iu=yh'e_0e_i\phi_{i0}\phi_{i0}^{-1}u=yh'(e_0e_ie_0)\phi_{i0}^{-1}u=y(e_0e_ie_0)h'\phi_{i0}^{-1}u=xe_0h'\phi_{i0}^{-1}u=x\phi_{i0}h'\phi_{i0}^{-1}u=xhu$となる．即ち$xuh=xhu$が示された．よってh∈𝒜(A)となり，H⊆𝒜(A)となる．また本定理の直前に記した性質より，𝒜(A)をXe_0に制限したものは，Hの部分群となり，H⊇𝒜(A)が示される．即ち，𝒜(A)＝Hとなって，定理が示された．　□

例　A＝(X, I, N)，X＝{1,2,3,4,5,6,7,8}，I＝{a,b,c}として状態遷移を表１の様に定める．

Aの状態遷移

	a	b	c
1	2	4	2
2	3	6	3
3	1	5	7
4	5	1	5
5	6	3	6
6	4	2	8
7	2	4	2
8	5	1	5

H'

	h_1'	h_2'	h_3'	h_4'	h_5'	h_6'
1	1	2	3	4	5	6
2	2	3	1	5	6	4
3	3	1	2	6	4	5
4	4	6	5	1	3	2
5	5	4	6	2	1	3
6	6	5	4	3	2	1

表１

$u\in I^*$に対するϕ_uを$\bar{u}$で表す．この時，$E_0=\{\bar{a}^3,\bar{c}^3\}$, $X\bar{a}^3=\{1,2,3,4,5,6\}$, $X\bar{c}^3=\{2,3,5,6,7,8\}$となり，$\bar{a}^3\mathcal{C}(A)\bar{a}^3$は$S_3$と同型である．eとして$\bar{a}^3$をとると，H'は表１の様に表される．基本分割は{{1,4},{2,3,5,6},{7,8}}となる．h_1, h_4を，$7h_1=7$, $8h_1=8$, $7h_4=8$, $8h_4=7$となる様にh_1'とh_4'を拡張したものとすれば，H＝$\{h_1,h_4\}$である．

４．むすび

本論文では，有限オートマトンの自己同型群について，半群論的立場から考察し，自己同型群の具体的構成に関連する新たな結果と，e𝒞(A)eと自己同型群の

新たな関係を３章において示した.

３章では強連結オートマトンAの自己同型群$\mathcal{A}(A)$に関する従来の結果を改善し，$\mathcal{A}(A)$は，$e\mathcal{C}(A)e$の中心化群の元で基本分割を固定する要素からなる群と同型になることを示した.

基本分割は自己同型群による分割よりは大きいものではあるが，Barnesが与えた自己同型群の分割の抽象的な条件とは異なり，実際の構成を示唆する具体的なものである.

文献

(1) Barnes B.H. : "On the Group of Automorphisms of Strongly Connected Automata", Math. Syst. Theory, 4, pp.289-294(1970).

(2) Bayer R. : "Automorphism groups and quotients of strongly connected automata and monadic algebras", IEEE Conf. Rec. 1966, 7th Ann. Symp. on Switching and Automata Theory(1966).

(3) Bavel Z. : "Introduction to the Theory of Automata", Reston Publishing Company(1983).

(4) Clifford A.H. and Preston G.B. : "The Algebraic Theory of Semi-Groups ", Math.Surveys No.7,Amer. Math. Soc., Providence, R.I., (1961).

(5) Fleck A.C. : "Isomorphism group of automata", J. Assoc. Compt. Mach 9, pp.469-476(1962).

(6) Fleck A.C. : "On the automorphism group of an automaton", J. Assoc. Compt. Mach 12, pp.566-569(1965).

(7) Holcombe W.M.L. : "Algebraic Automata theory", Cambridge University Press (1982).

(8) Perrin D. et Perrot J.-F. : "Congruences et Automorphismes des Automates Finis", Acta Inf., 1, pp.159-172(1971).

(9) Shibata Y. : "On the Structure of Abelian Automata", J. Comput. & Syst. Sci., 13, pp.143-152(1976).

(10) 植村憲治 : "Regular Permutation GroupとStrongly Connected AutomatonのAutomorphism Groupについて", 京都大学数理解析研究所講究録123 (1971).

(11) Uemura K. : "Semigroups and Automorphism Groups of Strongly Connectecd Automata", Math. Syst. Theory, 8, pp.8-14(1974).

(12) 植村憲治 : "Automorhphism group of a factor automaton II", 京都大学数理解析研究所講究録, 213 pp.239-248(1974).

(13) Wielandt H. : "Finite permutation groups", Academic Press, New York, (1964).

(14) Weeg G.P. : "The structure of an automaton and its operation-preserving transformation group", J. Assoc. Compt. Mach, 9, pp. 345-349(1962).

(15) Zassenhaus H. : "The Theory of Groups, 2nd ed.", Chelsea, New York (1949).